1 Equidistribution on compact groups

Let $X$ be a compact topological space. Let $C(X)$ be the space of continuous functions $X \to \mathbb{C}$; this is a Banach space under the supremum norm. Let $\mu$ be a measure on $X$, i.e., a continuous linear map $C(X) \to \mathbb{C}$ which is nonnegative (i.e., the integral of a function taking nonnegative real values is nonnegative) and of total measure 1.

A sequence $x_1, x_2, \ldots$ of elements of $X$ is equidistributed with respect to $\mu$ if for any continuous function $f$,

$$\int_X f \, d\mu = \lim_{N \to \infty} \frac{1}{N} \sum_{i=1}^{N} f(x_i).$$

2 Topological groups

The key example for us is when $X$ is a compact Lie group (e.g., a finite group), and $K$ is the space of conjugacy classes of $X$ (viewed with the quotient topology from $G$). In this case, $K$ has a unique translation-invariant measure with total measure 1, called the Haar measure; we use this measure on $X$ and on $K$.

**Theorem 1** (Peter-Weyl). With notation as above, the sequence $x_1, x_2, \ldots$ is equidistributed with respect to the Haar measure $\mu$ if and only if for any irreducible character $\chi : G \to \mathbb{C}$ of $G$,

$$\lim_{N \to \infty} \frac{1}{N} \sum_{i=1}^{N} \chi(x_i) = \int_X \chi \, d\mu.$$  

Note that the integral on the right is 1 if $\chi$ is the trivial character and 0 otherwise (orthogonality of characters).

3 $L$-functions and equidistribution

Here is a big generalization of our approach to Chebotarev’s density theorem. Take $K$ and $X$ as in the previous example. Let $x_1, x_2, \ldots$ be a sequence of elements of $X$, and let $x_i \to N(x_i)$ be a function whose values are all integers at least 2. We make the following additional hypotheses.
(i) Assume that the Euler product

$$\prod_i (1 - N(x_i)^{-s})^{-1}$$

converges absolutely for $\operatorname{Re}(s) > 1$, and extends to a meromorphic function on a neighborhood of $\operatorname{Re}(s) \geq 1$ with no zeroes or poles in $\operatorname{Re}(s) \geq 1$ except for a simple pole at $s = 1$.

(ii) Let $\rho$ be any irreducible representation of $K$ with character $\chi$. Put

$$L(s, \rho) = \prod_i \det(1 - \rho(x_i)N(x_i)^{-s})^{-1}.$$  

(Note that $\rho(x_i)$ is only defined up to conjugation.) Then $L(s, \rho)$ converges absolutely for $\operatorname{Re}(s) > 1$, and extends to a meromorphic function on a neighborhood of $\operatorname{Re}(s) \geq 1$ with no zeroes or poles in $\operatorname{Re}(s) \geq 1$ except possibly at $s = 1$.

**Theorem 2.** The number of $x_i$ with $N(x_i) \leq n$ is asymptotic to $n/\log n$ as $n \to \infty$. Moreover, for any irreducible character $\chi$ of $G$,

$$\sum_{i: N(x_i) \leq n} \chi(x_i) = c(\chi)n/\log n + o(n/\log n),$$

where $-c(\chi)$ is the order of vanishing of $L(s, \rho)$ at $s = 1$.

**Proof.** Yet another straightforward generalization of our original proof of the prime number theorem.

**Corollary 3.** Assume that there exists $c$ such that for any $n \in \mathbb{Z}$, there are at most $c$ values of $i$ with $N(x_i) \leq c$. Then the $x_i$ are equidistributed for Haar measure if and only if $c(\chi) = 0$ for every nontrivial irreducible character at $\chi$.

This reproduces the Chebotarev density theorem from the previous unit.

## 4 The Sato-Tate conjecture

The following is a rather nonobvious application of the above formalism.

**Conjecture 4** (Sato-Tate). Suppose $E$ does not have complex multiplication. Let $\alpha_p$ be the root of $x^2 - a_p x + p$ with nonnegative imaginary part. Then \(\arg(\alpha_p/\sqrt{p}) \) is equidistributed in $[0, \pi]$ for the measure $\frac{2}{\pi} \sin^2 \theta d\theta$.

What does the condition that $E$ does not have complex multiplication mean? The points of $E$ naturally form an abelian group, in which three points add to 0 if and only if they are collinear. We say $E$ has complex multiplication if the only endomorphisms of $E$ as an algebraic group are multiplication by integers. (Over $\mathbb{C}$, $E$ forms a Riemann surface which looks like the quotient of $\mathbb{C}$ by a lattice; an endomorphism of $E$ corresponds to a complex number which multiplies the lattice into itself.)
Theorem 5 (Clozel, Harris, Taylor). The Sato-Tate conjecture holds if $j(E) \notin \mathbb{Z}$. (This implies that $E$ does not have complex multiplication.)

I’ll skip the definition of the $j$-invariant $E$ for now; see Silverman’s book.

5 Equidistribution and Sato-Tate

How does the elliptic curve example relate to Sato-Tate? Put $K = SU(2)$, the group of $2 \times 2$ unitary matrices of determinant 1. Any class in $X$ contains a unique matrix of the form

$$\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}, \quad 0 \leq \theta \leq \pi.$$ 

Thus we may use the $\alpha_p$’s to generate elements $x_p$ of $X$ by taking $\theta = \arg(\alpha_p/\sqrt{p})$. The Haar measure on $X$ is precisely the Sato-Tate measure, so we are reduced to asking whether the $x_p$ are equidistributed.

The irreducible representations of $K$ are just the symmetric powers of the standard 2-dimensional representation. Hence Sato-Tate reduces to the following, which is the real hard content in the work of Clozel-Harris-Taylor. (Note that you have to shift the abscissa of absolute convergence by $1/2$.)

Theorem 6. Let $P_n(T)$ be the polynomial with constant coefficient 1 and roots $\alpha_p^n, \alpha_p^{n-1}, \ldots, \alpha_p$. If $j(E) \notin \mathbb{Z}$, then the Euler product

$$\prod_p P_n(p^{-s})^{-1}$$

extends to a holomorphic function on $\mathbb{C}$. (Since the Euler product converges absolutely for $\text{Re}(s) > 3/2$, the product cannot vanish for $\text{Re}(s) \geq 3/2$.)

Exercises (optional)

1. Let $\alpha_1, \ldots, \alpha_m$ be real numbers such that $1, \alpha_1, \ldots, \alpha_m$ are linearly independent over $\mathbb{Q}$. Apply Weyl’s criterion to prove that the sequence $x_n = (n\alpha_1, \ldots, n\alpha_m) \in (\mathbb{R}/\mathbb{Z})^m$ is equidistributed for the usual measure.

2. Prove that the sequence $\log n$ is not uniformly distributed for any measure on $\mathbb{R}/\mathbb{Z}$. 